The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications

Bustard, J. (2015). The Impact of EU Privacy Legislation on Biometric System Deployment: Protecting citizens but constraining applications. *IEEE Signal Processing Magazine*, *32*(5), 101-108. https://doi.org/10.1109/MSP.2015.2426682

Published in:
IEEE Signal Processing Magazine

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

The Impact of EU Privacy Legislation on Biometric System Deployment

I Introduction

Biometric systems provide a valuable service in helping to identify individuals from their stored personal details. Unfortunately, with the rapidly increasing use of such systems [1], there is a growing concern about the possible misuse of that information. To counteract the threat, the European Union (EU) has introduced comprehensive legislation [2] that seeks to regulate data collection and help strengthen an individual's right to privacy. This article looks at the implications of the legislation for biometric system deployment. After an initial consideration of current privacy concerns, it examines what is meant by 'personal data' and its protection, in legislation terms. Also covered are issues around the storage of biometric data, including its accuracy, its security, and justification for what is collected. Finally, the privacy issues are illustrated through three biometric use cases: border security, online bank access control and customer profiling in stores.

II Privacy Concerns with Biometrics

Many are now concerned about the possible misuse of biometric data [3, 4]. In 2006, for example, a telephone survey by the UK Information Commissioner's Office (Fig. 1) revealed that over 45% of respondents viewed biometric data as 'extremely sensitive' [4]. This was a higher percentage than for other forms of personal data that already carry strong legal protections, such as ethnic origin, political opinions, religious beliefs, and trade union membership.

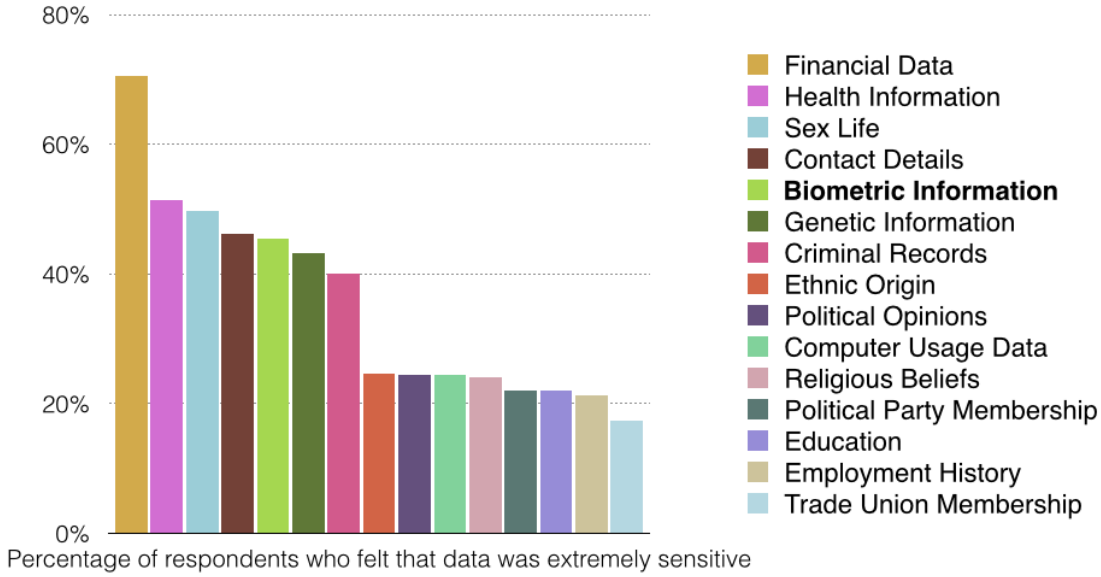

Figure 1: *Sensitivity ranking of personal data [4]*

Some privacy issues are specific to biometrics, such as concerns that:

- Biometric systems could be used to reveal medical conditions.
- Biometric use makes it easier to gather personal information, including the ability to do so covertly. For example, recent developments in biometrics at a distance [5] (Fig. 2) have increased the accuracy with which individuals can be identified remotely. Such technology is starting to be deployed commercially in security [6] and customer profiling applications [7].
- Biometrics could be used to link databases that have been anonymised yet still contain images of the individuals concerned. This is not necessarily an argument against the use of biometrics for identification, as much as a legitimate concern that de-anonymisation techniques should not be applied to subvert citizens' attempts to maintain their privacy.

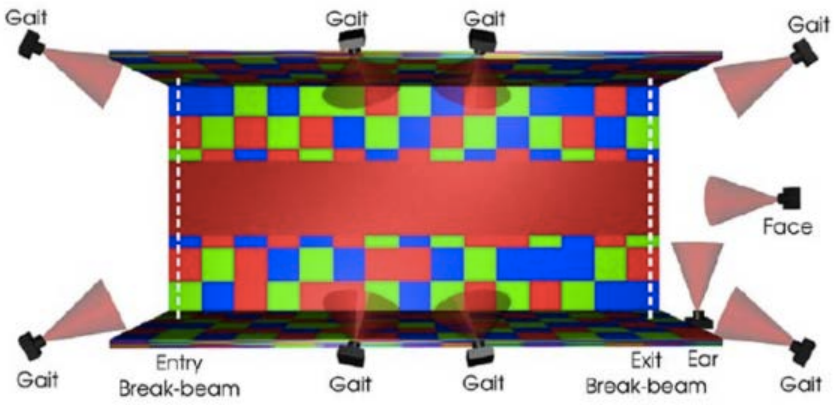

Figure 2*: An image from the Southampton Multi-biometric Tunnel [8]. The tunnel automatically recognises individuals passing through it using 3D gait, ear and face recognition. Such systems can have many applications but also raise significant privacy concerns as they have the potential to be deployed covertly.*

There are also psychological objections to biometric use, with some suggesting that measurements of a person's body are inherently more personal than other data about them [9]. Also in psychological terms, public resistance to the adoption of biometric technology is perhaps more a reflection of an understandable resistance to change rather than any substantial harm involved. For example, this is illustrated in recent discussions about the use of biometrics in schools where there was concern raised that such use could lead to “desensitisation” [10].

Concerns cover both public and private use of biometrics. Despite legal regulations on how personal data, including biometrics, can be used, there remain doubts over whether organisations can be trusted to follow such regulations. Moreover, national security services are typically exempt from these controls, provided internal governmental oversight committees agree their actions are proportional to the threat involved. In light of recent revelations about data collection by some security services [11], however, there are understandable doubts that such oversight is sufficient. Indeed, even when organisations do not actively attempt to abuse personal data, it is often difficult in practice for them to ensure its privacy, as illustrated by some of the well-publicised breaches of security that have occurred [12].

The concerns of the public are further heightened by the fact that biometrics are often used in situations where there is a significant asymmetry of power between those deploying the technology and those who will be monitored by it. Examples range from employers monitoring the time keeping of employees [13] to governments monitoring those entering and leaving their country.

Key Privacy Questions

- *What biometric data is being gathered and by whom?*
- *Is data being used solely for the purpose for which it was gathered?*
- *Is data accurate?*
- *Is data held securely?*
- *Is everyone operating within legal regulations?*
- *Are legal regulations sufficient?*
- *Are legal regulations proportionate to the threat posed to privacy?*

III. Legal Context

The growing concern over citizens' privacy has led to a number of changes in government legislation that will directly affect how biometric systems are deployed. In particular, the EU is in the process of introducing new data protection legislation [2] that will strengthen and unify existing laws in European member states. Significantly, the legislation also subjects companies outside the EU to the same data protection regulations if they offer services to EU citizens, or monitor their behaviour.

A. Definition of Personal Data

When personal data is gathered by biometric systems it is subject to data protection legislation. The new European Data Protection Regulation defines personal data as:

"any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his

physical, physiological, mental, economic, cultural or social identity."

In other words, if any data can be linked to an individual, it is 'personal'. This is intentionally broad and includes data such as the ip address of computers when such information can identify users uniquely [14]. Biometric data, both raw images and biometric templates, would clearly fall into this category, as they are inherently linked to a specific individual.

The EU also makes a distinction between personal data and *sensitive* personal data—which is information that relates to health, sex life, racial or ethnic origin, political opinions, religious or philosophical beliefs, and even trade-union membership. Because of the close connection between biometrics and the physical body, ethnic origin and a number of medical conditions can be inferred from some biometric data, making it 'sensitive' [15]. In particular, EU legislation explicitly mentions facial images as a form of sensitive personal data [16].

CCTV

Because the EU classifies facial images as sensitive personal data, this raises questions about the legitimacy of CCTV use, which frequently captures facial images without explicit consent. In a recent case, a Belgian court dealt with this issue by claiming that the data gathering itself is not processing [17]*. However, this is inconsistent with the privacy concerns on which the legislation is based. Sensitive data is protected because it could be used for discrimination. While gathering CCTV imagery is not necessarily discriminatory, hackers or feature creep could lead to discriminatory applications in the future. If so, then the Belgian ruling may well be challenged at some stage.*

B. Consent

In general, the processing, storage or transmission of sensitive personal data is not permitted. One important exception, however, is when explicit, free consent is given. This is convenient, for example, in applications such as unlocking a mobile phone.

However, the use of such applications is still conditional on: (i) sufficient data security being applied; (ii) the data not being used for other purposes or shared with third parties; and (iii) provision made for users to revoke their consent at any time.

Workplaces and commercial businesses are not typically required to obtain explicit free consent for technology they deploy. This is because it is argued that employees and customers can leave organisations when they are uncomfortable with their working practices, though in reality some may have little real choice.

Current methods of explicit consent often take the form of complex legal terms and conditions that are typically not understood fully by the person giving consent. Also, such terms often do not reflect actual privacy preferences but are simply accepted because the person giving approval believes that there is no reasonable alternative [18].

For many biometric applications, there will be an explicit enrolment stage where biometric features are recorded in a controlled way. This stage may be the appropriate point at which to obtain explicit consent. Biometrics technology can also be used to identify whether someone has agreed to biometric identification, as long as all biometric information is discarded if consent is not given [19].

C. Protection through Anonymity

One general approach to overcoming the limitations imposed by data protection legislation is to anonymise data. However, this is not an option for biometric systems. As noted in a report by a data protection committee for the council of Europe:

“with regard to biometric data, the option of making the data anonymous is not available as biometric data by their very nature, form an instrument to identify individuals, particularly when they are automatically processed” [20].

For EU law, the definition of 'identifiable' is so broad that data can be considered

personal if the data controller has any way of identifying the persons behind the data [21].

There are also obligations to implement data protection by ‘design and by default’ (Article 23) [2]. These design principles mean that biometric system designers are obliged to minimise the quantity of personal data that is collected and processed. They must also restrict the time that data is held and keep the number of individuals who have access to the data to a minimum. Existing analysis of default practices [22] indicate that most people will accept default settings. As a result, requiring explicit consent is likely to result in substantially reduced adoption of new biometric technologies.

One possible technical approach to anonymity is to use encryption methods to separate the storage of biometric templates from the system performing the verification [23]. This is done to ensure that the organisation that stores the templates is unaware of which verification transactions are occurring and in turn that the organisation verifying an identity cannot access the personal biometric template. Such an approach would not necessarily avoid the necessity for consent as the initial storage of biometrics would require user permissions, as would any processing performed using such data. However, users may find that such an approach is more acceptable to them than trusting a single organisation with all of their data. Such anonymisation techniques are still at a research stage, however, and so are unlikely to form a legal requirement. However, once practical commercial implementations become available, data protection authorities may interpret them as ‘data protection by design’ requirements.

D. Protection through Aggregate Statistics

Biometric technology can also be used to create aggregated statistics as, for example, in recognising the number of unique visitors to a store. In this way, biometric systems can help automate business intelligence gathering that has

historically been performed manually. This aggregated usage data is typically anonymous, referring only to total numbers of unique individuals rather than individual usage patterns. This does not address the privacy issues of using biometric information itself but does limit how much information is linked to a specific individual.

It is currently permissible in the EU to obtain categorisation information about a person, as long as that information is not itself personally identifiable, and the information is not combined in a way that can make it personally identifiable. However, the new regulation includes restrictions on the use of categorisation data for profiling purposes:

“Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour” (Article 20) [2].

This would restrict the use of so-called *soft biometrics* [24], which identify broad features of an individual, such as their age, sex or race. The systems involved do not gather uniquely identifiable biometric signatures and so could provide demographic information about customers without identifying them. However, there are situations where soft biometric data may be sufficient to identify an individual uniquely and so may also be problematic in relation to the legislation.

E. Biometric Data Retention Issues

There are a number of data protection issues associated with the storage of personal data. In particular, the ensured accuracy, security, control and proportionality of that storage areespecially important.

Data Accuracy

Stored personal data must be accurate. The European Data Protection Regulation states in Article 5 that personal data must be:

"(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (Article 5) [2].

Biometric signatures can change and thus any biometric system needs a means of updating biometric templates. In particular, ageing has a significant effect on many biometrics [25].

Data Security

The General European Data Protection Regulation states that:

"The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation" (Article 23) [2].

The regulation also states that further acts may be passed for the purpose of specifying the criteria for achieving these standards.

Organisations, such as Europise [26], provide certification of products and IT services to ensure that a sufficiently high standard of data security is in place. Such standards have a strong emphasis on internal organisational measures, including an assurance of the physical security of stored data, and providing authentication and logging facilities to ensure that only authorised processing is performed. However, the numerous data breaches that have occurred suggest that either these measures are insufficient within large organisations or that they are difficult to enforce in practice.

In addition to these general data security measures a number of technologies designed specifically for securing biometric templates have been developed and this continues to be an active area of research [27]. The precise methods required for securing biometrics have not been made explicit within the law. In practice they will be determined by judgements based on advice from experts. The subsequent rulings will then provide a precedent for what security measures are required.

Data Control

The new regulation emphasises the rights of individuals to control the information that is stored about them. Those gathering personal data, including data that could be used for biometric analysis, must clearly inform those affected that the data is being collected, and explain how it will be used (Article 5) [2]. They must also provide a means to identify the information already stored and enable those affected to adjust that information if it is inaccurate. In addition, citizens have the right to object to such data processing, requiring it to cease unless organisations can demonstrate "*compelling legitimate grounds*" (Article 19) [2]. This is a significant change of emphasis from previous legislation where processing was permissible unless citizens could find a legitimate reason for it to stop. The reversal moves the focus of biometric technology use from situations in which *it may be beneficial*, to situations in which *it is evidently needed*.

Data Collection Proportionality

The new Data Protection Regulation allows for the use of biometrics without consent provided certain conditions are met. In particular, it is possible to process personal data where it is in the substantial public interest and where requiring consent would undermine the effectiveness of its use. For example, this includes the prevention or detection of crime (Article 2) [2] and journalistic investigation (Article 80) [2]. This means that for many security applications, biometric use would still be possible. However, in such cases the data processing must be:

“(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed” (Article 5) [2].

In addition, for it to be used legitimately, biometrics must be judged *proportional* to the application [28]. For example, the widespread use of biometric systems in schools within the UK was challenged by the EU commission on grounds of proportionality, which resulted in a requirement for parental consent and alternative identification methods being made available [29].

One consideration in assessing proportionality is whether a less invasive alternative approach could be used. As biometrics is considered a potential threat to privacy this ruling, in effect, means that biometrics is only proportional when no reasonable alternative identification method exists, which imposes a significant bias against the use of biometric technology. This restriction seems out of step with the treatment of other workplace practices, such as the use of time-keeping machines, which may have similar negative associations but are not limited by legislation in the same way. In many cases, biometrics is used as a convenient alternative to a door key or identity card, and so perhaps should be treated in a similar way.

IV. Use Cases for Biometrics

Biometrics can be applied in a variety of different circumstances and each brings with it different concerns and legislative constraints. This section aims to highlight these differences with three example use-cases.

Border Security

Figure 3*: Biometric passports are being widely adopted throughout the EU*

All countries carefully monitor the identity of individuals passing through their borders. These checks identify suspected security threats and help prevent illegal immigration. Biometrics technology offers a means to automate this process as well as potentially increasing the accuracy of identifying those claiming a false identity.

From an ethical perspective, it is important that any such automated system be suitable for the diverse range of users it is likely to process, from babies to wheelchair users. No section of the population should experience undue inconvenience or unjustified discrimination because of their specific needs.

In addition to automating routine identification checks, biometric systems can also be used to monitor a 'watch-list' of individuals who are a particularly high security risk. Such individuals are likely to be travelling with false identification papers that may pass existing inspection methods.

Consent: Where biometrics are applied as a cost saving automation measure, biometric use may be optional. This often takes the form of a 'fast-track' route through border control. However, where biometrics are applied as a means to improve the accuracy of identification, such as with the US-VISIT program [30],

biometric checks will be mandatory.

Accuracy: When Biometric Systems are used to automate passport control, an alternative verification method is needed. This is due to the potential for a false negative verification match as well as the likelihood of processing citizens who have missing or damaged biometric features. For example, fingerprints can be obscured by manual work.

Security: Public bodies have significant oversight, and in some cases have freedom of information legislation that would facilitate investigation of abuses of data protection. This is generally not possible in the private sector, where such investigations would reveal commercially sensitive information. However, in the case of border control there are significant security issues. As a result, the operation of the technology is likely to be secret and thus it falls to whistle-blowers to reveal potential abuses by government.

Another factor crucial to the privacy of users is whether biometric information is held on a centralised database or carried with the user, such as on a biometric passport. Each additional link in processing or data storage carries with it an increased risk that it may be compromised by hackers or that feature creep by one of the organisations involved will lead to further invasions of privacy. Similar concerns can arise if biometric data is transmitted to a third party to perform verification tests. To some extent, modern encryption methods can mitigate these concerns, but they do not remove them as all solutions rely on some degree of trust.

However, even without a centralised biometric database, the introduction of identity papers with biometric information can potentially introduce significant privacy issues. If the biometric data is accessible via a remote wireless connection there is a risk that passports could be compromised by a hacker with a nearby sensor. Likewise, such passports would require an enrolment system which itself may involve a number of third parties, each of which could be compromised or could introduce privacy

invading features in the future.

Proportionality: Border security focuses on preventing serious criminal and terrorist activity and, as a result, it is considered legitimate to partially invade individual privacy if doing so preserves the higher priority of preventing harm. However, if biometrics are used in watch-list applications there are further concerns. In particular, such applications raise the question of proportionality. Specifically, on what grounds should border security be permitted to automatically identify an individual and subject them to increased scrutiny? Also, because of the potential seriousness of watch-list false matches the accuracy of biometric identification needs to be considered—particularly in light of the case of Brandon Mayfield who was held for over two weeks on terrorism charges, partly because of a single false match to a fingerprint obtained from bomb parts [31]. In addition, preventing an individual from leaving a country is a serious restriction on their freedom and a common abuse of governmental powers against critics [32].

Online Bank Account Access Control

Figure 4*: Small portable devices with fingerprint readers can be used to provide time-linked passwords to secure online services.*

Bank transactions are increasingly being performed using online applications that enable the monitoring of accounts and the transfer of funds. However, there is a

significant risk that criminals may use these systems to steal from the accounts involved. Biometrics is one way to improve the security of online banking. Specifically, in conjunction with existing security systems, biometrics can be used to provide *two-factor identification*. This can take the form of a combination of something that is known, say a password, with someone's biometric signature, based on a physical feature. Other factors can also be used to further enhance security such as the MAC address of the user's PC.

Consent: It seems reasonable to assume implied consent where customers have the option of moving to another bank that doesn't require biometric security. Under the new data protection regulation, however, explicit free consent requirements mean that implied consent is insufficient.

Security: As with passport control, the privacy of the system is affected by whether biometric information can be kept locally. This is possible, for example, by using a fingerprint scanner to unlock a device owned by the customer that produces a secure, time-linked password for accessing a remote banking website. Some biometrics, such as voice, however, may require biometric templates to be stored on a server.

Proportionality: In EU law, verification applications, where a user claims an identity which is verified, are considered less invasive than recognition applications where a user is compared against a large database to determine identity. However, unless free consent is provided, such technology may well be viewed as disproportionate if alternative security methods are available. An individual bank may view biometrics as a more secure alternative, but the final decision would rest with the courts.

Customer Profiling

Figure 5*: Using soft biometrics, advertising billboards can detect the numbers, genders and age groups of viewers in an area. This helps retailers understand how shoppers are affected by advertising and promotions.*

Although the use of biometrics has traditionally been associated with security applications, there are many other circumstances where the automated recognition of individuals is valuable. One commercially important area is in tracking customers while they shop, primarily to help understand their interests, and hence identify ways to sell them more goods and services (Fig. 5). The current technology used for customer tracking in physical spaces is similar to the initial tracking capabilities of web analytics companies, focusing on counting the number of unique visitors and identifying statistics of where customers travel within stores.

Consent: One form of consent is through the use of a loyalty card, which already tracks customer behaviour through monitoring their purchases. However, not everyone uses a loyalty card and some are concerned about being monitored in this way.

Another form of monitoring is through the tracking of the unique identifier transmitted

by a customer's smart phone. Here companies typically try to obtain consent by using an opt-out policy, posting signs to inform customers that they are being monitored [33]. This approach is controversial, however [34], and would no longer be permissible under the new EU regulations if any of the gathered data were categorised as personal.

Security: To facilitate tracking across different locations it may be necessary to share biometrics between different sites. If a centralised database is used, this will increase concerns about the security of the data. There is also likely to be a market for user profile information, similar to how such data is used for online profiling of customers. Current legislation would require strong contractual constraints on such data, particularly if any of it is identified as being sensitive.

It is likely that there would also be commercial advantage in extending monitoring to provide similar levels of information to that available via online profiling. Such profiling includes the acquisition of demographic information, such as age and gender [35]. Recent developments in soft biometrics [24] could be used to estimate some of this additional information but the new regulation is likely to greatly restrict these applications unless explicit free consent has been given.

Conclusions

This article started by acknowledging public concern about the possible abuse of the personal data that biometric systems collect and store. This set the context for identifying the main measures introduced by the new European Data Protection Regulation to control data collection and help strengthen a citizen's rights to privacy and data protection. The discussion first clarified what is meant by 'personal data' in the legislation, before considering its use in protecting that data. Protection included a consideration of the legislation relating to the accuracy and security of the data held, justification for what is collected, and the option of individuals providing 'consent' to data use. The privacy issues associated with biometrics were illustrated

through a consideration of three biometric use cases: border security, online banking and customer tracking in stores.

Biometrics is frequently given as an example of a technology which raises privacy concerns and, as has been shown in this article, there are significant legislative restrictions applied to its use.

In general, it is desirable to limit the complexity and application of legal restrictions as they will consume valuable time and resources. Also, increased complexity of the law further isolates citizens from the legal process and can create a situation where only those who can afford specialised legal services can understand when they are acting legitimately. EU data protection regulation can be interpreted as focusing on minimising personal data collection. Further work is needed to identify if the harms that such legislation prevent are adequately balanced against the potential gains made possible by the new technology.

The overall conclusion is that the new EU regulation will significantly increase the protection of each citizen's privacy. However, it is also likely to limit the adoption of biometric technology, particularly in workplaces and in commercial organisations.

Author

John Bustard (j.bustard@qub.ac.uk). Dr John Bustard is a lecturer at Queens University Belfast in the Speech, Image and Vision Systems Research Group. He has over seven years research experience in Biometrics, including work on the Tabula Rasa European Framework 7 project investigating the vulnerability of biometrics to spoofing attacks; he is currently a UK expert for the ISO group contributing to the WD5 30107 standard on Presentation Attack Detection. He also has a keen interest in ethics. This has led to invited presentations on the ethics of biometrics and surveillance for the Centre for Science, Society and Citizenship and for NESTA. He is currently the chairman of an ethical advisory group for the

European Framework 7 research projects ISAR+ and SOTERIA. More broadly, he is a co-investigator on the Centre for Secure Information Technologies Phase 2 EPSRC project, which is concerned with securing the internet of things.

REFERENCES

[1] Article 29 data protection working party, “Opinion 03/2012 on developments in biometric technologies,” April 2012.

[2] European Commission, “Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)”, 2012. [Online]. Available: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011

[3] A. Krupp, C. Rathgeb, C. Busch, "Social acceptance of biometric technologies in Germany: A survey," *International Conference of the Biometrics Special Interest Group (BIOSIG)*, pp.1-5, Sept. 2013

[4] K. McCullagh, “Data Sensitivity: Proposals for Resolving the Conundrum,” *Journal of International Commercial Law and Technology*, Vol. 2, Issue 4, 2007

[5] M. Tistarelli, S. Z. Li, R. Chellappa, “Handbook of Remote Biometrics for Surveillance and Security,” *Advances in Computer Vision and Pattern Recognition*, 2009

[6] “Surveillance, persistent observation and target recognition(spotr).” 2014. [Online]. Available: http://www.spotrtech.com/

[7] S. Harris. “Computer to shopstaff: Vip approaching,” 2013. [Online]. Available: http://www.thesundaytimes.co.uk/sto/news/uknews/Tech/article1287590.ece

[8] R. D. Seely, S. Samangooei, M. Lee, and J. N. Carter, M. S. Nixon, "The University of Southampton Multi-Biometric Tunnel and introducing a novel 3D gait dataset", *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems*, pp. 1-6, Sept. 2008.

[9] J. D. Woodward, K. W. Webb, E. M. Newton, M. A. Bradley, D. Rubenson, K. Larson, J. Lilly, K. Smythe, B. Houghton, H. A. Pincus, J. Schachter, P. S. Steinberg, "Army Biometric Applications: Identifying and Addressing Sociocultural Concerns," Rand Corporation.

[10] A. Ramasastry, “Biometrics in the School Lunch Line: Why Parents Should Be Concerned About the Privacy Implications of This Trend,” [Online]. Available: https://verdict.justia.com/2012/10/09/biometrics-in-the-school-lunch-line

[11] S. Landau, "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations", *IEEE Security & Privacy*, vol. 11, no. 4, pp. 54-63, 2013

[12] PriceWaterhouseCoopers, “The global state of information security,” Survey 2014. [Online] Available at: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

[13] Biometric Attendance Systems. [Online] Available at: http://www.alldaytime.co.uk/

[14] Scarlet v. SABAM Case C-70/10. [Online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62010CJ0070

[15] E. Mordini, "Biometrics, human body, and medicine: A controversial history," *Ethical, Legal, and Social Issues in Medical Informatics,* Medical Information Science Reference, 2008.

[16] Project group on Data Protection, “Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data,” 2005.

[17] P. De Hert, O. De Schutter, S. Gutwirth, “Pour une réglementation de la vidéosurveillance,” *Journal des tribunaux*, pp. 569-579, 21 Sept. 1996.

[18] E. Luger, S. Moran, T. Rodden, "Consent for all: revealing the hidden complexity of terms and conditions," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* pp. 2687-2696, 2013.

[19] Article 29 data protection working party, “Opinion 02/2012 on facial recognition in online and mobile services,” 2012.

[20] Y. Liu, "Identifying Legal Concerns in the Biometric Context," *Journal of International Commercial Law and Technology*, Vol. 3, No. 1, 2008.

[21] P. de Hert, “Biometrics: legal issues and implications,” *Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission, 2005.

[22] C. W. Park, S. Y. Jun, D. J. MacInnis, "Choosing What I Want Versus Rejecting What I Do Not Want: An Application of Decision Framing to Product Option Choice Decisions," *Journal of Marketing Research*, Vol. 37, No. 2, pp. 187-202, 2000.

[23] N. D. Sarier, “A Survey of Distributed Biometric Authentication Systems,” *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, Sept. 2009.

[24] D. Reid, S. Samangooei, C. Chen, M. Nixon, and A. Ross, “Soft biometrics for surveillance: an overview,” *Machine Learning: Theory and Applications*, pp. 327-352, 2013.

[25] M. Fairhurst, “Age Factors in Biometric Processing,” IET Digital, 2013

[26] EuroPriSe. [Online] Available at: www.european-privacy-seal.eu

[27] A. K. Jain, K. Nanakumar, A. Nagar, "Biometric template security," *Eurasip Journal on Advances in Signal Processing*, 2008.

[28] Office of the Privacy Commissioner of Canada, “Data at your fingertips: Biometrics and the Challenges to Privacy,” Feb. 2011.

[29] UK Department for Education, “Protection of Biometric Information of Children in Schools,” 2012. [Online] Available at: https://www.gov.uk/government/publications/protection-of-biometric-information-of-

children-in-schools

[30] L. Amoore, "Biometric borders: Governing mobilities in the war on terror," *Political geography*, Vol. 25, No. 3, pp. 336-351, 2006.

[31][39] Mayfield v. US, No. 07-35865. FindLaw. Dec. 2009.

[32] C. Harvey, R. P. Barnidge. "Human rights, free movement, and the right to leave in international law," *International Journal of Refugee Law,* Vol. 19, No. 1, pp. 1-21, 2007.

[33] Future of Privacy Forum, “Mobile location analytics code of conduct,” 2013 [Online]. Available: http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf

[34] P. Cohan, "How nordstrom uses wifi to spy on shoppers," 2013. [Online]. Available: http://www.forbes.com/sites/petercohan/2013/05/09/how-nordstrom-and-home-depot-use-wifi-to-spy-on-shoppers/

[35] Google, "Overview of demographics and interests reports," 2014. [Online].Available: https://support.google.com/analytics/answer/2799357